IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re application of Rosario Gennaro November 20, 2006

Serial Nbr: 09/753,727 Filed: January 3, 2001

For: Method, System and Computer Program Product for Efficiently Generating Pseudo-Random Bits

Art Unit: 2131 Examiner: Matthew T. Henning

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a Response to the Notification of Non-Compliant Appeal Brief mailed November 1, 2006, which stated that the Summary of Claimed Subject Matter is defective in Appellant's Appeal Brief filed on August 23, 2006 (hereinafter, "Appellant's previously-filed Appeal Brief"). In accordance with MPEP §1205.03, titled "Non-Compliant Appeal Brief and Amended Brief", a replacement **Summary of Claimed Subject Matter** is provided herewith, and this replacement **Summary** should be substituted for paragraphs 1 - 11 of Appellant's previously-filed Appeal Brief.

5) SUMMARY OF CLAIMED SUBJECT MATTER

1. Appellant's independent Claim 1 specifies elements of "computer-readable program code means for providing an input value comprising C random bits [Specification, p. 16, lines 10 - 12]" (Claim 1, lines 3 - 4); "computer-readable program code means for generating an output sequence comprising N pseudo-random bits [Specification, p. 16, lines 15 - 17] using the provided C-bit input value as a short exponent x [Specification, p. 16, lines 15 - 16 and 18 - 19] of a 1-way function G**x mod P [Specification, p. 16, line 6; p. 17, lines 1 - 4; p. 18, lines 12 - 13; p. 20, lines 6 - 7; **Fig. 3**, first rectangular box; and **Fig. 4**, first rectangular box] that comprises modular exponentiation modulo a safe N-bit prime number P [Specification, p. 17, lines 1 - 2], wherein a base G of the modular exponentiation is a fixed generator value [Specification, p. 17, lines 2 - 3]" (Claim 1, lines 5 - 8); "computer-readable program code means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion [Specification, p. 16, lines 15 - 17; p. 20, lines 7 - 10; **Fig. 3**, "bit selector" box; and **Fig. 4**, "bit selector" box]" (Claim 1, lines 9 - 10); and "computer-readable program code means for using the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the computer-readable program code means for generating [Specification, p. 16, lines 15 - 16] while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits [Specification, p. 16, lines 16 - 17], until a desired number of pseudo-random output bits have been generated [Specification, p. 20, lines 12 - 15]" (Claim 1, lines 11 - 15).

1.1 In other words, to summarize Claim 1 in a concise manner, an N-bit output is iteratively generated, and of these N bits, "C" of them are used as input to a next iteration while the other (N

- C) bits are output for forming a pseudo-random value.

1.2 Independent Claim 13 specifies elements of "means for providing an input value comprising C random bits [Specification, p. 16, lines 10 - 12]" (Claim 13, line 3); "means for generating an output sequence comprising N pseudo-random bits [Specification, p. 16, lines 15 - 17] using the provided C-bit input value as a short exponent x [Specification, p. 16, lines 15 - 16 and 18 - 19] of a 1-way function G**x mod P [Specification, p. 16, line 6; p. 17, lines 1 - 4; p. 18, lines 12 - 13; p. 20, lines 6 - 7; **Fig. 3**, first rectangular box; and **Fig. 4**, first rectangular box] that comprises modular exponentiation modulo a safe N-bit prime number P [Specification, p. 17, lines 1 - 2], wherein a base G of the modular exponentiation is a fixed generator value [Specification, p. 17, lines 2 - 3]" (Claim 13, lines 4 - 7); "means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion [Specification, p. 16, lines 15 - 17; p. 20, lines 7 - 10; **Fig. 3**, "bit selector" box; and **Fig. 4**, "bit selector" box]" (Claim 13, lines 8 - 9); and "means for using the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the means for generating [Specification, p. 16, lines 15 - 16] while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits [Specification, p. 16, lines 16 - 17], until a desired number of pseudo-random output bits have been generated [Specification, p. 20, lines 12 - 15]" (Claim 13, lines 10 - 13).

1.3 In other words, to summarize Claim 13 in a concise manner, an N-bit output is iteratively generated, and of these N bits, "C" of them are used as input to a next iteration while the other (N - C) bits are output for forming a pseudo-random value.

1.4 Appellant's independent Claim 25 specifies elements of "providing an input value comprising C random bits [Specification, p. 16, lines 10 - 12]" (Claim 25, line 3); "generating an output sequence comprising N pseudo-random bits [Specification, p. 16, lines 15 - 17] using the provided C-bit input value as a short exponent x [Specification, p. 16, lines 15 - 16 and 18 - 19] of a 1-way function G**x mod P [Specification, p. 16, line 6; p. 17, lines 1 - 4; p. 18, lines 12 - 13; p. 20, lines 6 - 7; **Fig. 3**, first rectangular box; and **Fig. 4**, first rectangular box] that comprises modular exponentiation modulo a safe N-bit prime number P [Specification, p. 17, lines 1 - 2], wherein a base G of the modular exponentiation is a fixed generator value [Specification, p. 17, lines 2 - 3]" (Claim 25, lines 4 - 7); "separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion [Specification, p. 16, lines 15 - 17; p. 20, lines 7 - 10; **Fig. 3**, "bit selector" box; and **Fig. 4**, "bit selector" box]" (Claim 25, lines 8 - 9); and "using the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the generating step [Specification, p. 16, lines 15 - 16] while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits [Specification, p. 16, lines 16 - 17], until a desired number of pseudo-random output bits have been generated [Specification, p. 20, lines 12 - 15]" (Claim 25, lines 10 - 13).

1.5 In other words, to summarize Claim 25 in a concise manner, an N-bit output is iteratively generated, and of these N bits, "C" of them are used as input to a next iteration while the other (N - C) bits are output for forming a pseudo-random value.

1.6 Appellant's independent Claim 39 specifies elements of "means for providing an input

value comprising C random bits [Specification, p. 16, lines 10 - 12]" (Claim 39, line 2); "means for generating an output sequence comprising N pseudo-random bits [Specification, p. 16, lines 15 - 17] using the provided C-bit input value as a short exponent x [Specification, p. 16, lines 15 - 16 and 18 - 19] of a 1-way function G**x mod P [Specification, p. 16, line 6; p. 17, lines 1 - 4; p. 18, lines 12 - 13; p. 20, lines 6 - 7; **Fig. 3**, first rectangular box; and **Fig. 4**, first rectangular box] that comprises modular exponentiation modulo a safe N-bit prime number P [Specification, p. 17, lines 1 - 2], wherein a base G of the modular exponentiation is a fixed generator value [Specification, p. 17, lines 2 - 3]" (Claim 39, lines 3 - 6); "means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion [Specification, p. 16, lines 15 - 17; p. 20, lines 7 - 10; **Fig. 3**, "bit selector" box; and **Fig. 4**, "bit selector" box]" (Claim 39, lines 7 - 8); "means for using the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the means for generating [Specification, p. 16, lines 15 - 16] while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits [Specification, p. 16, lines 16 - 17], until a desired number of pseudo-random output bits have been generated [Specification, p. 20, lines 12 - 15]" (Claim 39, lines 9 - 12); and "means for using the desired number of generated pseudo-random [output] bits as input to an encryption operation" [see Specification, p. 20, lines 15 - 16, which further describes the output bits as "keying material" for the encryption operation; see also Specification, p. 9, lines 12 - 13; p. 10, lines 7 - 8; and p. 11, lines 6 - 7] (Claim 39, lines 13 - 14).

1.7 In other words, to summarize Claim 39 in a concise manner, an N-bit output is iteratively generated, and of these N bits, "C" of them are used as input to a next iteration while the other (N

- C) bits are output for forming a pseudo-random value, and the pseudo-random value formed from the output bits may be used as input (e.g., as "keying material") to an encryption operation.

2. Appellant's independent Claim 52 specifies elements of "providing an N-bit input value in which (N-C) uppermost contiguous ones of the bits are all set to zeroes [Specification, p. 16, lines 10 - 12] and in which C lowermost contiguous ones of the bits are random [Specification, p. 16, lines 10 - 12]" (Claim 52, lines 3 - 4); "generating an output sequence comprising N pseudo-random bits [Specification, p. 16, lines 15 - 17] using the provided N-bit input value as an effectively-short, C-bit exponent x [Specification, p. 16, lines 15 - 16 and 18 - 19] of a 1-way function G**x mod P [Specification, p. 16, line 6; p. 17, lines 1 - 4; p. 18, lines 12 - 13; p. 20, lines 6 - 7; **Fig. 3**, first rectangular box; and **Fig. 4**, first rectangular box] that comprises modular exponentiation modulo a safe N-bit prime number P [Specification, p. 17, lines 1 - 2], wherein a base G of the modular exponentiation is a fixed generator value [Specification, p. 17, lines 2 - 3]" (Claim 52, lines 5 - 8); "separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion [Specification, p. 16, lines 15 - 17; p. 20, lines 7 - 10; **Fig. 3**, "bit selector" box; and **Fig. 4**, "bit selector" box]" (Claim 52, line 9 - 10); "creating a new N-bit input value in which the (N-C) uppermost contiguous ones of the bits are all set to zeroes [Specification, p. 16, lines 11 - 12; p. 20, lines 9 - 10] and in which the lowermost C contiguous ones of the bits are set to the C-bit portion [Specification, p. 16, lines 15 - 16; p. 20, lines 9 - 10]" (Claim 52, lines 11 - 13); and "using the new N-bit input value as the provided input value for a next iteration of the generating step [Specification, p. 16, lines 14 - 16] while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits [Specification, p.

16, lines 14 - 17, and in particular, lines 16 - 17], until a desired number of pseudo-random output bits have been generated [Specification, p. 20, lines 12 - 15]" (Claim 52, lines 14 - 17).

2.1 In other words, to summarize independent Claim 52 in a concise manner, an N-bit output is iteratively generated, and of these N bits, the lowermost "C" contiguous ones of them are used as input to a next iteration while the uppermost (N - C) contiguous ones of the bits are output for forming a pseudo-random value. (While not specifically stated in Claim 52, these output bits may be used, for example, as input to an encryption operation).

3. Dependent Claims 2, 14, 26, and 40 specify "wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption" [Specification, p. 10, lines 8 - 9; p. 17, lines 14 - 16; p. 18, lines 3 - 4; p. 19, line 18 - p. 20, line 1; Abstract, third sentence].

4. Dependent Claims 6, 18, 30, and 44 specify "wherein C = 160 and N = 1024" [Specification, p. 17, lines 10 - 13; p. 19, line 8] whereas Dependent Claims 7, 19, and 32 specify "wherein C is greater than or equal to 160 and N is greater than or equal to 1024 [Specification, p. 17, lines 10 - 13] " (or "at least", rather than "greater than or equal to", in Claim 19).

5. Dependent Claims 9, 21, 34, and 47 specify "wherein the (N-C)-bit portion is concatenated to pseudo-random output bits previously generated by the [generator]" [Specification, p. 20, lines 12 - 14].

6. Dependent Claims 10, 22, and 35 specify "wherein the (N-C)-bit portion is a contiguous group of (N-C) bits from the generated N-bit output sequence [Specification, p. 20, lines 9 - 10; **Fig. 4**, noting "bits 1 - 864" are a contiguous (N-C)-bit group of bits]". Dependent Claims 11, 23, and 36 specify "wherein the (N-C)-bit portion is a non-contiguous group of (N-C) bits from the generated N-bit output sequence [Specification, p. 20, lines 9 - 10]".

7. Dependent Claims 12, 24, and 37 specify "further comprising ... using the desired number of generated pseudo-random bits as input to an encryption operation [Specification, p. 9, lines 12 - 13; p. 20, lines 15 - 16]".

8. Dependent Claims 48 - 51 specify "wherein N is greater than or equal to (C * 6) [Specification, p. 17, lines 10 - 13, noting that when C = 160, C * 6 = 960 and N = 1,024; p. 19, line 8]".

9. Independent Claims 1, 13, and 39 and dependent Claims 12 and 24 include means plus function terminology. Structure, material, or acts supporting this terminology are described in Appellant's specification, as will now be described.

10. With regard to the "means for providing" element of independent Claims 1, 13, and 39, the text on p. 6, lines 10 - 12 of Appellant's specification describes use of hardware for generating random seeds (e.g., the "C" random bits referred to in the "means for providing"), and p. 15, lines 6 - 7 refer to an alternative that comprises implementing the present invention in hardware (or a

combination of hardware and software). For the "means for generating" element of independent Claims 1, 13,and 39, refer to (*inter alia*) **Fig. 3** and the corresponding text on p. 20, lines 3 - 7. With regard to the "means for separating" element of independent Claims 1, 13, and 39, refer to (*inter alia*) **Figs. 3 - 4** and the corresponding text on p. 20, lines 7 - 11. The "means for using the C-bit portion" element of independent Claims 1, 13, and 39 is described by (*inter alia*) the text on p. 20, lines 11 - 15.

10.1 With regard to the "means for using the desired number" element of independent Claim 39, see **Fig. 1**, which depicts a computer workstation **10**, and see also the corresponding text in Specification, p. 12, lines 4 - 15. See also Specification p. 9, lines 12 - 13 and p. 20, lines 15 - 16.

11. The "means for using the desired number" element in dependent Claims 12 and 24 is described, for example, by text on p. 20, lines 15 - 17.

REMARKS

As noted above, a replacement **SUMMARY OF CLAIMED SUBJECT MATTER** is provided herein, and this replacement **SUMMARY** is to be substituted for the **SUMMARY** in Appellant's Appeal Brief filed on August 23, 2006 (hereinafter, "Appellant's previously-filed Appeal Brief").

In addition, a typographical error has been detected in paragraph 50 of Appellant's previously-filed Appeal Brief. Paragraph 50 of Appellant's previously-filed Appeal Brief cites **Section 7.2.1** thereof (".. for the same reasons discussed above in **Section 7.2.1** with regard to independent Claims 13, 25, and 39 ..."). Instead of **Section 7.2.1**, Paragraph 50 should refer to **Section 7.2.2**. Appellant apologizes for this typographical error.

Respectfully submitted,

/Marcia L. Doubet/ /#40,999/

Marcia L. Doubet,
Attorney for Appellant
Reg. No. 40,999

Customer Number for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587